УДК 004.056

DDOS ATTACKS AND THEIR FORECASTING

Milanin A. V., Smolkov M. I, Tolstova T. V.

Samara National Research University, Samara

DDoS (Distributed Denial of Service) attacks have recently attracted a lot of attention among researchers, IT professionals and public at large as they constitute a menace for corporate sites, e-commerce, banking services, etc. and therefore are able to cause enormous financial losses by precluding people's access and exchange important information [1].

The underlying principle of DDoS attacks is bringing down networks, Web-based applications and services by overwhelming them with too much data acting from multiple different sources. They are designed to target any aspect of business including disabling a specific computer, service or an entire network; impairing the work of alarms, printers, phones or laptops; hitting system resources like bandwidth, disk space, processor time or routing information; executing malware that affects processors and triggers errors in computer microcodes; exploiting operating system vulnerabilities to drain system resources; and crashing the operating system [2].

DDoS attacks can be broadly divided into three categories:

1. Application Layer attacks: They target HTTP in an attempt to exhaust the resource limits of internet services. Examples include Zero-day DDoS attacks and attacks geared towards OpenBSD and Apache vulnerabilities.

2. Protocol attacks: The cyber-criminal conducts the attack with the aim to saturate service resources of the targets or of firewalls, load balancers, and other intermediate communication equipment. It exploits network protocol to abuse the victim's resources. Examples include Smurf attacks and SYN Floods.

3. Volume based attacks: The aim is to saturate the victim's bandwidth. Examples include ICMP flood and other spoofed-packet traffic floods.

There has been extensive research on preventing DDoS attacks and mitigating their affects [1, 3]. The authors suggest such techniques as disabling unused services, installing the latest security patches, disabling IP broadcast, using firewalls, and IP hopping. However no specific solution for preventing the attacks completely has been found so far.

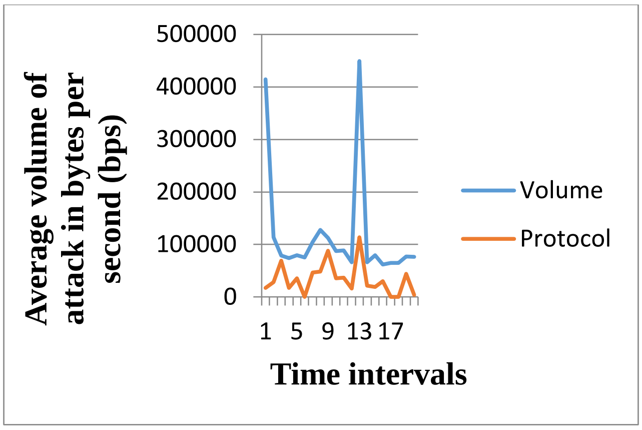

Fig.1. History and future of DDoS attacks

On the X axis - Time intervals for which was measured the average volume of attacks in bytes per second – Y axis.

One of the ways to minimize the damage could be forecasting the contingency using statistics which can be found at *Digital Attack Map* – a live data visualization of DDoS attacks around the globe which surfaces anonymous attack traffic data to let users explore historic trends and find reports of outbreaks happening on a given day [4]. Using this tool makes it possible to predict future tends of attacks. Figure 1 shows that the highest peak was in 2013 both in terms of volume and protocol, whereas future outrage (though not so dramatic) can be expected in 2019.

References

1. Behal S., Kumar K. Trends in Validation of DDoS Research [Text] // International Conference on Computational Modeling and Security (CMS 2016). Procedia Computer Science. 2016. Volume 85 (2016). Pp. 7–15.

2. Minhas K. A Study on High Rate Shrew DDOS Attack [Text] // International Journal of Advancements in Technology. 2015. Volume 6. Pp. 1-6.

3. Prasad K.M., Reddy A.R., Rao K.V. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey [Text] // Global Journal of Computer Science and Technology: E Network, Web & Security. 2014. Volume 14. Issue 7. Pp. 1-19.

4. Digital Attack Map [online source]. Available from: <http://www.digitalattackmap.com/about/> (Accessed June 2017).